

Catching the Fakes

Applying neural networks to images helps identify counterfeit goods.

COUNTERFEITING IS A big business. Nearly \$509 billion of fake and pirated products were sold internationally in 2016. In that year, the latest for which data was available, counterfeit goods made up 3.3% of international trade, up from 2.5% three years earlier, according to the Organization for Economic Cooperation and Development.

That figure, which does not include domestic trade in fakes, not only means companies are losing revenue and consumers are not getting their money's worth; counterfeiting also helps fund organized crime. It exploits low-wage laborers. Because it skirts safety regulations, makers of counterfeits could use toxic materials or produce unsafe products.

Now, companies are turning to artificial intelligence (AI) to help them identify counterfeit products and stanch the flow of faux goods.

Amazon, for instance, launched Project Zero in 2019. Makers of products provide the company with data about their logos, trademarks, and other features, and Amazon's machine learning algorithm scans listings on the company's website and automatically removes those it deems fake.

Other companies have rolled out tools to allow retailers to identify fakes using smartphones with scanning attachments.

"Counterfeit goods are among the leading causes of a lot of bad things," says Lakshminarayanan Subramanian, a professor of computer science at New York University and co-founder and chief scientist at Entrupy, a New York-based company founded in 2012 that uses AI to verify the authenticity of luxury goods.

The company's system works with microscopic images of the goods in question, looking for features that are common to an authentic product but not to a fake. Those features could be in the texture of the material, the stitching, a zipper, or the way a logo has been stamped into an item. The leather of a



luxury handbag, for instance, will have what appear to be peaks and valleys when viewed at a microscopic scale.

Entrupy trains its AI starting with images of an area of handbags, both authentic and counterfeit, and breaks that image into smaller chunks. It then applies bag-of-words, a technique developed for natural language processing that sorts words by their frequency in a text and uses that to make inferences about the text. In the case of handbags, the "words" are small areas of structural features that might repeat or vary from place to place across the material. The computer creates a histogram showing the frequency of these visual words and how that frequency differs between real and fake goods.

Based on the results, the company then decides which regions of the product are important for identifying whether the product is authentic, and performs Deep Learning on that data, using a convolutional neural network, noted for its efficiency at image recognition.

Selecting the right features on which to train the neural network turned out to be important in order to reduce the number of false positive results, explains Ashlesh Sharma, a former student of Subramanian's who is now chief technology officer at Entrupy. "If you just threw in a bunch of images to a Deep Learning model, the output at times is completely random. Even the best of the Deep Learning models would have an accuracy of 80% or something," Sharma says.

The company offers a money-back

guarantee if it labels an item as authentic and it turns out to be counterfeit, so 80% or so is not a high-enough accuracy rate. To push that up to greater than 99%, Entrupy will test a handbag on a series of models, using 10 to 12 regions of the bag. That creates a set of probability scores as to whether the bag is authentic. If the average score of all the models is high enough, they label the bag as real; if it is too low, they do not declare the bag a fake, but say they are unable to authenticate it.

Small Differences

Part of the trick of confirming whether a product is real or counterfeit is not simply to focus on just one type of feature, but to check, say, the quality of the stitching or how the logo looks, as well as the texture of the material. That way, even if a counterfeiter managed to steal a shipment of matching leather, there would still be differences that would give away the fake.

The other important consideration is that the features being examined should be smaller than what a counterfeiter could manufacture, so the company usually focuses on structures between 5 and 10 micrometers in size. "If you can nanofabricate a bag, you might be able to produce similar geometries, but luxury goods in particular are not nanofabricated," Subramanian says. "So it's sort of a challenge between what the magnification at which we capture images is, and what the manufacturing inaccuracy of these specific items is."

Users—usually stores selling luxury

brands such as Prada or Louis Vuitton, or warehouses transferring products from manufacturers to retail outlets—can purchase an attachment for smartphones to enable them to take a series of microscopic images, following a set of instructions from an app on the phone. They upload the images to Entrupy, which checks them against their AI models and delivers a verdict. The whole process takes just minutes, but the company is looking for ways to streamline it.

Entrupy also works with sellers of sneakers, a product sector in which limited editions can sell for hundreds of dollars. Entrupy's technology could be used on other goods that have identifiable features, Sharma says, and they have done some work authenticating expensive watches. The system is less effective with reflective surfaces, such as jewelry or porcelain, because stray light adds artifacts to the image that confounds the AI. Sharma says using infrared light may reduce that issue. The system could also be useful for detecting fake pharmaceuticals or counterfeit money, but Subramanian says the company has not yet ventured into those markets because of the complexity of regulations governing them.

Working with Light

Adding another layer of data allows IBM's Crypto Anchor Verifier to handle a wider range of products. Like Entrupy, it, too, requires a scanner to be attached to a smartphone, so it also can gather images and compare microscopic features to determine what is real and what is not. In addition, though, it looks at the waveforms of light reflecting from or passing through the object being scanned.

One smartphone attachment has a slot into which a vial containing a liquid or powder can be inserted. Donna Dillenberger, a fellow at IBM's Thomas J. Watson Research Center, demonstrated by displaying two vials of olive oil—one pure, one extra virgin. To the human eye, they are nearly identical yellow fluids. She slips one into the holder, and in a few seconds the phone's screen displays a graph describing the wavelengths of passing through it. She replaces it with the other, and a very different graph appears. "Even though to the human eye the liquids look the same, to the Verifier they look different," she says. "We've done the same things to

Like Entrupy, IBM's product relies on convolutional neural networks to train the computer to distinguish features of actual products from those of fakes.

authenticate wines, between expensive and inexpensive wines."

The Verifier also can distinguish chemotherapy drugs, or discover whether expensive cosmetics have been adulterated with cornstarch. The work on powders was prompted by a scandal in 2008, when powdered milk and baby formula from China was found to have been laced with melamine, which was used to dilute milk to stretch sales, and wound up sickening children.

Like Entrupy, IBM's product relies on convolutional neural networks to train the computer to distinguish features of actual products from those of fakes. Because wines and oils are easy to differentiate, the algorithm needed only a handful of samples, in the "low double-digits," to train on, Dillenberger says. For more complicated tasks, such as grading diamonds by how they refract light, she said, thousands of samples were necessary.

The combination of imaging and AI also can be applied to integrated circuits and circuit boards, says Domenic Forte, a professor of electrical and computer engineering at the University of Florida. Forte trained a neural network to identify physical defects that reveal if a chip has been altered, such as scratches or variations in surface texture that come from resurfacing a chip or changing its marking. "If the counterfeiter changes the marking from commercial to industrial grade, they could sell you a part that's much cheaper and it won't withstand what your application requires," Forte says.

Visual inspection of ICs currently is performed manually, but Forte hopes

to automate the process. Using infrared imaging allows the system to see through a part's packaging and look for alterations underneath. There are electrical tests that can be used to verify parts, but they are often specific to a part, making them more difficult to automate, and they can require expensive equipment, Forte says. Sometimes they even require packaging to be removed, destroying the part in the process.

For all of AI's ability to catch fake goods, Dillenberger wonders whether there might not be a larger societal question that is going unaddressed. "You could build these technologies to catch things, but how could we nudge people, who must be extremely talented to even make counterfeits in the first place, to do something else with their gifts?" she asks. "Why aren't they being rewarded to make something that's not counterfeited? How can technology help at that systemic problem?"

Further Reading

Asadizanjani, N., Tehranipoor, M., and Forte, D. Counterfeit Electronics Detection Using Image Processing and Machine Learning, *J. of Physics: Conf. Series* 787 (2017) <https://iopscience.iop.org/article/10.1088/1742-6596/787/1/012023>

Sharma, A., Srinivasan, V., Kanchan, V., and Subramanian, L. The Fake vs Real Goods Problem: Microscopy and Machine Learning to the Rescue, *KDD '17*, (2017) <https://dl.acm.org/doi/10.1145/3097983.3098186>

Balagurusamy, V., Siu, V., Kumar, A.D., Dureja, S., Ligan, J., Kudva, P., Tong, M., and Dillenberger, D. Detecting and discriminating between different types of bacteria with a low-cost smartphone based optical device and neural network models, *SPIE 2019 Nanoscience and Engineering Conference Proceedings*, (2019) <https://spie.org/Publications/Proceedings/Paper/10.1117/12.2529829?SSO=1>

Cheung, M., She, J., and Liu, L. Deep learning-based online counterfeit-seller detection, *IEEE Conf. on Computer Communications Workshops*, (2018) <https://ieeexplore.ieee.org/document/8406896>

Entrupy Authentication Demo Video <https://www.youtube.com/watch?v=HMXQJK7v9t8>

Neil Savage is a science and technology writer based in Lowell, MA, USA.